UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/437,352	11/09/1999	DIMITRI KANEVSKY	YO999-411	7851

7590   07/01/2005

KEVIN M MASON
RYAN MASON & LEWIS LLP
1300 POST ROAD
SUITE 205
FAIRFIELD, CT 06430

EXAMINER
STULBERGER, CAS P

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

MAILED

Application Number: 09/437,352
Filing Date: November 09, 1999
Appellant(s): KANEVSKY ET AL.

JUL 0 1 2005

Technology Center 2100

Kevin M. Mason
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/11/2005.

(1)   ***Real Party in Interest***

A statement identifying the real party in interest is contained in the brief.

(2)   ***Related Appeals and Interferences***

A statement identifying the related appeals and interferences which will directly affect or

be directly affected by or have a bearing on the decision in the pending appeal is contained in the

brief.

(3)   ***Status of Claims***

The statement of the status of the claims contained in the brief is correct.

(4)   ***Status of Amendments After Final***

The appellant's statement of the status of amendments after final rejection contained in

the brief is correct.

(5)   ***Summary of Invention***

The summary of invention contained in the brief is correct.

(6)   ***Issues***

The appellant's statement of the issues in the brief is correct.

(7)   ***Grouping of Claims***

The rejection of claims 1-58 stand or fall together because appellant's brief does not

include a statement that this grouping of claims does not stand or fall together and reasons in

support thereof. See 37 CFR 1.192(c)(7).

(8)   ***Claims Appealed***

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9)   ***Prior Art of Record***

6,219,793 B1   Li   4-2001

5,757,916   MacDoran   5-1998

Meyer, "Wireless Enhanced 9-1-1 Service - Making it a Reality," Bell Labs Technical Journal;

Autumn 1996

(10)   ***Grounds of Rejection***

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11, 13, 15-21, 24, 26-32, 35, 37-39, 40-47, 49, and 50-57 above are rejected

under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,219,793 B1 to Li et al. and

further in view of U.S. Patent No. 5,757,916 to MacDoran et al.

In regards to claims 1, 5, 15-16, 26, 27, 37-39, 40-47, 49, and 50-57, Li discloses a

system and a method for employing a user's fingerprint to authenticate a wireless

communication. When a wireless communication is to be initiated, the central authentication

system engages in a challenge-response authentication with the wireless phone using the stored

fingerprint associated with the mobile identification number (MIN) (Li: Abstract). Li also

discloses that biometric data other than fingerprints can be used such as a user's voice (Li:

column 17, lines 29-35).

However Li does not disclose a challenge response method that uses the location.

MacDoran discloses that the state vector attributes distilled from the state vector observations supplied to the host authentication server define the location of the client, and that location is compared to the particular predefined location information for that client stored in the database. If the host authentication server produces a remote client location that matches the previously registered client location within a predetermined threshold, access is granted to the remote client user (MacDoran: column 24, lines 12-15).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of using biometric data to authenticate wireless communications as disclosed by Li with the method of providing the location of the client and compared it to the stored location value and granting access to the user if the location is within a predetermined threshold as disclosed by MacDoran in order to make "spoofing" the host device very difficult (MacDoran: column 1, lines 15-16).

In regards to claim 2, Li discloses requesting a personal identification number (PIN) each time a call is made. This meets the limitation of a "password."

In regards to claims 3, 4, 10, 21, 32, Li does not disclose a pocket token or computer readable card.

MacDoran discloses using access tokens (MacDoran: column 1, lines 40, 49). This meets the limitation of "wherein said response is a computer readable card" or "pocket token."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the wireless cellular phone as disclosed by Li with the method of

using access tokens as disclosed by MacDoran in order to determine whether a person or device

attempting to access or perform a transaction with a host computer system is a person or device

entitled to access, most host computer systems require the person or device to provide

information confirming identity (MacDoran: column 1, lines 21-25).

In regards to claims 6-9, 11, 13, 17-20, 24, 28-31, and 35, Li does not however disclose

using a global positioning system.

MacDoran discloses using a Global Position System (GPS) sensor to determine the

location of the singnature provided by the remote client. This meets the limitation of "wherein

said global positioning system includes a local verification system."

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to combine the wireless cellular phone as disclosed by Li with the global

positioning system as disclose by MacDoran in order to determine the location of an object or

person with great precision and accuracy (MacDoran: column 5, lines 41-43).

Claims 12, 14, 22, 23, 25, 33, 34, 36, 48, and 58 are rejected under 35 U.S.C. 103(a) as

being unpatentable over U.S. Patent No. 6,219,793 B1 to Li et al. in view of U.S. Patent No.

5,757,916 to MacDoran et al applied to claims 1-11, 13, 15-21, 24, 26-32, 35, 37-39, 40-47, 49,

and 50-57 above, and further in view of "Wireless Enhanced 9-1-1 Service - Making it a

Reality," Bell Labs Technical Journal (Autumn 1996) by Meyer et al.

In regards to claims 12, 14, 23, 25, 34, 36, 48, and 58, Li does not disclose using 911

techniques or querying the user about something at the location of a requested device or facility.

Meyer however discloses asking the user of the cell phone "Do you have any more details on your location?" (Meyer: page 189, right column, lines 1-2).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the wireless cellular phone as disclosed by Li with the method of querying the user as to where they are because the existing E9-1-1 service was originally designed to support wireline calls from fixed locations (Meyer: page 188, right column, second paragraph).

In regards to claims 22 and 33 Li does not however disclose using triangulation.

Meyer however discloses that triangulation methods can be used (Meyer: page 198, left column).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the wireless cellular phone as disclosed by Li with the method of using triangulation as disclosed by Meyer because it can be implemented at a relatively low additional cost (Meyer: page 196, right column, third paragraph, last line).

(11)   Response to Argument

Applicant argues that MacDoran does not disclose "identifying a location of an authorized person associated with said response; identifying a location where said response is received; and providing access to said user if said locations match" as in independent claims 1, 16, 27, and 38. Claims 1, 16, 27, and 38 disclose "identifying a location of an authorized person associated with said response; identifying a location where said response is received; and

providing access to said user if said locations match." "Identifying a location of an authorized person associated with said response" is interpreted as meaning that the user has already been authorized prior to identifying a location of the user with a response. Li discloses a system and a method employing a user's fingerprint to authenticate a wireless communication (Li: Abstract, lines 1-2). This meets the limitation of "an authorized person." MacDoran discloses supplying state vectors to a server, which define the location of the client. This meets the limitation of "identifying a location where said response is received." The location is then compared to the predefined location information for that client to a list of authorized client locations stored there. This meets the limitation of "identifying a location of an authorized person associated with said response." If the locations match within a predetermined threshold, access is granted to the remote client user (MacDoran: column 24, lines 12-21). Li discloses authorizing a user, while MacDoran discloses a method of access control by using location of the user.

Applicant argues that MacDoran does not "require identifying each registered person within a predefined distance of said requested device." MacDoran discloses that the host authentication server produces a location which is compared against the previously registered client location. If the locations are within a certain threshold of each other, which could be millimeters up to several meters, then access is granted to the remote client user (MacDoran: Column 24, lines 18-29). The user at the client location meets the limitation of a "registered person" and the threshold between the locations meets the limitation of the "predefined distance of said requested devices."

Applicant argues that MacDoran does not disclose "identifying said user by comparing a location of each identified potential user with a location where said biometric information was

obtained." MacDoran discloses that predefined location information for clients is stored in a database (MacDoran: column 24, line 15-16). The list of predefined location information for clients meets the limitation of "a location of each identified potential user." MacDoran also discloses sending the state vectors to the host authentication server which defines the location of the client (MacDoran: column 24, lines 12-14). This meets the limitation of " the location where said biometric information was obtained."

Applicant argues that MacDoran does not disclose "identifying said user and confirming said user requesting access to said device is physically present at the location of said requested device by determining a location of said transmitting device (wherein said transmitting device is associated with said user)." MacDoran discloses that in order to determine whether a person attempting to access a host computer is in fact entitled to access the computer, most systems require the person to confirm their identity. One possible way of authenticating a user as known in the art is through a personal characteristic such as biometric characteristics including fingerprints, voice prints, retinal scans, etc (MacDoran: column 1, lines 21-25, 50-55). These methods are known in the art to authenticate a user who has to be physically present at the device in order to present their biometric characteristics.

Applicant argues that "even if each user is capable of having a separate GPS device, MacDoran does not disclose or suggest that each user has or should have a separate GPS device." The LSS unit, which produces the state vectors used in determining the location of the user, can exist in may different forms. The LSS may exist as a PC card form, such as a PCMCIA card format for laptop computer use in a remote client. It can be configured into a single chip for integrating into original equipment manufactured products (MacDoran: column 15, lines 43-47).

MacDoran discloses that each user who wants to access the host authentication server supplies state vectors, which defines their GPS location. Along with MacDoran disclosing that the LSS exists in a PCMCIA card format for laptop computer use in remote client and that it can also be configured onto a single chip for integrating into original equipment manufactured products suggests that each user has their own GPS device.

Applicant argues that "such techniques cited by the Examiner as being disclose by MacDoran (passwords, PIN's, and biometric authentication) are techniques for attempting to authenticate an individual person. The tests cited by the Examiner, however, can falsely authenticate an individual who is actually an impostor, as would be apparent to a person of ordinary skill in the art." Applicant gives an example of using a user having an artificial limb, which is used to authenticate that user. Applicant then gives the scenario that an impostor can acquire such an artificial limb and/or user's password and may access the electronic device while the authorized user is at another location. Applicant's are irrelevant since applicant is arguing limitations which are not disclosed in the claims. MacDoran discloses biometric authentication which meets the limitation of authenticating an individual person.

Applicant argues that MacDoran "does not disclose or suggest a system that can authenticate and individual user." MacDoran discloses user authentication by having the person confirm their identity by methods such as passwords, PINs, biometric authentication, etc (MacDoran: column 1, lies 21-55). All these systems are known in the art to be able to authenticate an individual user.

Applicant argues that "MacDoran discloses identifying the location of the remote client machine, not identifying the location of an authorized user." MacDoran discloses that the

location of the client attempting to access the host authentication server is identified (MacDoran:

column 24, lines 12-25). It is interpreted that in order for the remote client machine to attempt to

access the host authentication server that a user needs to be present in order to instruct the remote

client machine to access the host authentication server. MacDoran also discloses user

authentication through means such as biometric authentication (MacDoran: column 1, lies 21-

55). In order for the user to biometrically authenticate the user needs to be present at the remote

client machine. In either case the client is present at the machine and the location of the machine

is the location of the authorized user and meets the limitations.

Applicant argues that MacDoran does not disclose "comparing a location of each

identified potential users," but instead "only discloses comparing a location of a client machine."

MacDoran discloses comparing the received location with a previously registered client location.

MacDoran also discloses the authentication criteria is stored in a database (MacDoran: column

24, lines 3-29). It is interpreted that in order to find the potential user's stored location data, the

database will have to compare the received data to the data in the database in order to find the

potential user's location data. This meets the limitation of "comparing a location of each

identified potential users," but instead "only discloses comparing a location of a client machine."

Applicant argues that "biometric authentication systems may falsely authenticate a user;"

therefore, "the authorized user may not be at the location where the biometric authentication is

performed even if the biometric authentication (falsely) confirms the user's identity." This

argument is irrelevant since MacDoran discloses biometric authentication which is used to

authenticate a user at a device able to take biometric samples. Such device is known to be

located at the location which the user requests access.

Applicant argues that "dependent claims 6, 17, and 28 require wherein said location of an authorized person is obtained using an individual global positioning system" and "MacDoran does not disclose that a GPS is associated with a user." Applicant also argues that "dependent claims 43 and 53 require wherein said location of each identified potential user is obtained by the location of an individual global positioning system associated with each of said identified potential users." The LSS which supplies the state vectors to the authentication server, can exist as a PC card form, such as a PCMCIA card format for a laptop computer used in a remote client or as a single chip integrated on original equipment manufactured products (MacDoran: column 15, lines 43-47). It is interpreted that the laptop or the original equipment is used by a particular user to access the authentication server and is therefore associated with a user.

Applicant argues that "dependent claims 40 and 50 require wherein said step of identifying each registered person within a predefined distance of said requested device further comprises the step of identifying individual global positioning systems associated with registered persons within said predefined distance." MacDoran discloses that the remote client location that matches the previously registered client location within a predetermined threshold (eg. three meters).

Applicant argues that "dependent claims 13, 24, 35, 44, and 54 require wherein said location of an authorized person is obtained by identifying the location of a transmitting device associated with said authorized person. The GPS device disclosed by MacDoran is a receiving device, as would be apparent to a person of ordinary skill in the art." MacDoran discloses the LSS at the client provides the state vectors that are used in the authentication process

(MacDoran: column 23, lines 26-29). The LSS is therefor a transmitting device and meets the limitations.

Applicant argues that "dependent claims 41 and 51 require wherein said step of identifying each registered person within a predefined distance of said requested device further comprises the step of identifying individual global positioning systems associated with registered persons within said predefined distance." MacDoran discloses that the remote client location that matches the previously registered client location within a predetermined threshold (eg. three meters).

Applicant argues that "Meyer does not disclose or suggest identification of a user as described in the limitation of the independent claims." MacDoran meets these limitations as disclosed above and thusly this argument is not persuasive.

Applicant argues that "Meyer does not disclose obtaining the location of an authorized person using enhanced cellular 911 techniques." Meyer discloses using GPS technology that is integrated into cell phones in the future instead of TDOA or DOA triangulation methods to determine the location of the cell phone user because GPS is more accurate (Meyer: page 198, right column, first full paragraph; page 199-200). This meets the limitation of obtaining the location using enhanced 9-1-1 techniques.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

CS
June 23, 2005

Conferees
Gilberto Barron
Matthew Smithers

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

KEVIN M MASON
RYAN MASON & LEWIS LLP
1300 POST ROAD
SUITE 205
FAIRFIELD, CT 06430